Криптосистема с открытым ключом с использованием некоммутативных примитивов на базе алгебры Клиффорда

Н.А. Коковихина[a], С.В. Тихомиров[a], А.Н. Леухин [a]

[a]*Марийский государственный университет, 424000, пл. Ленина 1, Йошкар-Ола, Россия*

Аннотация

Предлагается способ шифрования с открытым ключом на основе метода с использованием некоммутативного криптографического примитива на базе алгебры Клиффорда. Разработана криптосистема с открытым ключом, основанная на использовании некоммутативных конечных групп и свойствах алгебры Клиффорда. Алгеброй Клиффорда задаются правила генерирования элементов группы и выполнения групповой операции умножения. Алгоритм шифрования применяется к многомерным векторам четных размерностей.

Ключевые слова: криптография; криптосистема с открытым ключом; шифрование; криптографический примитив; некоммутативная группа; алгебра Клиффорда

1. Введение

Широкое применение информационных технологий практически во всех областях общественной деятельности обуславливает критическое значение обеспечения информационной безопасности, что влечет необходимость применения механизмов защиты и контроля целостности информации и непрерывного их совершенствования. Алгоритмические средства защиты информационных технологий, базирующиеся на современной криптографии, являются не только гибкими и эффективными, но также лежат в основе информационных технологий, связанных с обработкой юридически значимых документов и сообщений.

Среди получивших распространение средств защиты информации выделяют системы криптографической зашиты информации, системы электронной подписи и другие системы, предназначенные для качественного и безопасного владения информацией и ее использования. Все эти системы реализуются по тем или иным алгоритмам защиты данных. Так, например, из алгоритмов симметричного шифрования часто применяются AES, DES, IDEA, ГОСТ 28147-89; из алгоритмов шифрования с открытым ключом - RSA, Elgamal, схема Рабина; а также алгоритмы электронной подписи, такие как схема Эль-Гамаля (Elgamal), RSA-PPS, DSA, ECDSA, ГОСТ Р 34.10-2012. С ростом вычислительных мощностей подобные алгоритмы должны оперировать все большими значениями и постоянно увеличивать длину используемого ключа, а подбор подходящих значений злоумышленником становится вопросом времени и использующейся вычислительной мощности.

Развитие в области высокопроизводительных вычислений, а также появление алгоритмов решения трудных задач не дает гарантий в безопасности использования современных криптографических алгоритмов, что актуализирует разработку новых методов шифрования для хранимой и передаваемой информации и усовершенствование тех, что используются на данный момент. Национальный институт стандартов и технологий (NIST) в декабре 2016 года официально зарегистрировал запрос в Федеральном Реестре [1] на поиск постквантовых алгоритмов с открытым ключом, обозначив надвигающуюся угрозу для большинства традиционных криптосистем защиты информации, которые опираются на проблемы факторизации целых чисел или задачи дискретного логарифмирования. NIST планирует заменить три существующих криптографических стандарта, которые могут быть наиболее уязвимыми с точки зрения воздействия криптографических вычислений — FIPS 186-4, NISTSP 800-56A и NISTSP 800-56B [2].

В этой работе рассмотрена криптосистема с открытым ключом с использованием некоммутативных примитивов на базе алгебры Клиффорда.

2. Криптосистема с открытым ключом на базе алгебры Клиффорда

Основными требованиями, предъявляемые к криптографическим алгоритмам и протоколам, которые используются в качестве алгоритмических механизмов защиты информации, являются их стойкость и безопасность. Они определяются вычислительно трудными задачами, лежащими в их основе, уровнем развития теории, методов и алгоритмов решения задач данного типа. Наиболее широко применяемые криптографические схемы с открытым ключом имеют практическую стойкость и безопасность, но не имеют теоретически доказанной стойкости.

Приведенная в работе криптосистема предназначена для шифрования и дешифрования данных, для подписи сообщения и проверки подписи с использованием некоммутативных примитивов на базе алгебры Клиффорда. Данная криптосистема опирается на вычислительно трудную задачу, формируемую над конечными некоммутативными группами. Трудность задачи заключается в поиске сопрягающего элемента в некоммутативных группах, т.е. вычисления элемента X из уравнения

$$Y = X * G * X^{-1},$$

где Y и G – известные элементы некоторой некоммутативной группы. Эта задача имеет доказанную сверхполиномиальную сложность, так как она сводится к решению задачи дискретного логарифмирования в циклической подгруппе некоммутативной группы [3].

2.1 Определение алгебры Клиффорда

Определим понятие алгебры Клиффорда.

Пусть E – векторное (линейное) пространство над полем комплексных чисел C, n – натуральное число и размерность поля E равна 2^n. Пусть в E введен базис $e, e^a, e^{a_1 a_2}, \dots, e^{1\dots n}$, где $a_1 < a_2 < \cdots$, (всего их 2^n), занумерованный упорядоченными мультииндексами длины от 0 до n. Индексы $a, a_1, a_2, \dots$ пробегают значения от 1 до n.

Пусть p и q – положительные целые числа и $p + q = n, n \geq 1$. Введем диагональную матрицу η размера n:

$$\eta = \|\eta^{ab}\| = diag(1, \dots, 1, -1, \dots, -1),$$

у которых на диагонали стоят p штук +1 и q штук -1.

Введем на E операцию Клиффордова умножения $U, V \to UV$ по следующим правилам:

1. дистрибутивность и согласованность с линейной структурой для любых $U, V, W \in E$ и $\alpha, \beta \in F$;
2. ассоциативность для любых $U, V, W \in E$;
3. унитальность для любого $U \in E$, т. е. $Ue = eU = U$;
4. унитальность для всех $a, b = 1, \dots, n$, т. е. $e^a e^b + e^b e^a = 2\eta^{ab} e$;
5. унитальность для всех $1 \leq a_1 < \cdots < a_k \leq n$, т. е. $e^{a_1} \dots e^{a_k} = e^{a_1 \dots a_k}$.

Тогда введенная таким образом алгебра называется алгеброй Клиффорда и обозначается CL(p,q).

Любой элемент U алгебры Клиффорда CL(p, q) представляется в виде разложения по базису:

$$U = ue + u_a e^a + \sum_{a_1 < a_2} u_{a_1 a_2} e^{a_1 a_2} + \cdots + u_{1\dots n} e^{1\dots n},$$

где $u, u_a, u_{a_1 a_2}, \dots, u_{1\dots n}$ – комплексные числа [4].

В качестве криптографического примитива для предложенной криптосистемы с открытым ключом используются некоммутативные группы на основе многомерных векторов четных размерностей. Алгебра Клиффорда позволяет задавать в качестве элементов группы гиперкомлексные числа любых размерностей, равных степенях с основанием 2 (т.е. размерности 4, 8, 16, 32, и т.д.), путем формирования правила выполнения умножения гиперкомплексных чисел. Очевидно, что для каждой новой размерности элемента группы правило выполнения групповой операции будет отличаться от всех предыдущих и будет уникальных. Данный факт позволяет также усложнить подбор ключей злоумышленником за счет увеличения мощности группы и, следовательно, возможных вариантов ключей.

Рассмотрим вектора с размерностями 4, 8 и 16.

2.2 Четырехмерные числа как элементы группы

Для четырехмерных чисел можно построить восемь различных таблиц умножения на базе алгебры Клиффорда, из них четыре являются некоммутативными.

На основе следующих базисных элементов алгебры Клиффорда были получены некоммутативные таблицы умножения для четырехмерных чисел:

1. $e_1^2 = 1,\ e_2^2 = 1,\ e_{1,2}^2 - 1;$
2. $e_1^2 = 1,\ e_2^2 = -1,\ e_{1,2}^2 - 1;$
3. $e_1^2 = -1,\ e_2^2 = 1,\ e_{1,2}^2 - 1;$
4. $e_1^2 = -1,\ e_2^2 = -1,\ e_{1,2}^2 - 1.$

Построим таблицу умножения для четырехмерных чисел на базе алгебры Клиффорда. Пусть базисные элементы $e_1^2,\ e_2^2,\ e_{1,2}^2$ алгебры Клиффорда равны (-1, -1, -1), тогда элементы таблицы будут иметь следующие значения, которые отражены в таблице 1:

1. $e_1 * e_2 = 1;$
2. $e_1 * e_{1,2} = e_1 * e_1 * e_2 = -e_2 = -1;$
3. $e_2 * e_1 = -e_1 * e_2 = -1;$
4. $e_2 * e_{1,2} = -e_2 * e_2 * e_1 = e_1 = 1;$
5. $e_{1,2} * e_1 = -e_2 * e_1 * e_1 = e_2 = 1;$
6. $e_{1,2} * e_2 = e_1 * e_2 * e_2 = -e_1 = -1.$

При генерации некоторого примитива q, используя любую из четырех некоммутативных таблиц умножения, и при существовании для q обратного элемента q^{-1} было обнаружено, что при осуществлении операции некоммутативного умножения $C = q * m^e * q^{-1}$, гарантируется восстановление исходного сообщения $m = q^{-1} * C^d * q$, где e и d являются взаимно обратными числами по некоторому модулю n, т.е. $e * d \equiv 1\ (mod\ n)$.

Таблица 1. Таблица умножения с базисными элементами алгебры Клиффорда (-1, -1, -1)

•	e_0	e_1	e_2	e_{12}
e_0	1	1	1	1
e_1	1	-1	1	-1
e_2	1	-1	-1	1
e_{12}	1	1	-1	-1

2.3 Восьмимерные числа как элементы группы

Для восьмимерных чисел возможно построить 64 различных таблиц умножения на базе алгебры Клиффорда (60 некоммутативных).

В качестве примера были выбраны следующие комбинации базисных элементов алгебры Клиффорда:

1. $e_1^2 = -1, e_2^2 = -1, e_3^2 = -1, e_{1,2}^2 = -1, e_{1,3}^2 = -1, e_{2,3}^2 = -1;$
2. $e_1^2 = 1, e_2^2 = 1, e_3^2 = 1, e_{1,2}^2 = -1, e_{1,3}^2 = 1, e_{2,3}^2 = 1;$
3. $e_1^2 = 1, e_2^2 = 1, e_3^2 = 1, e_{1,2}^2 = 1, e_{1,3}^2 = 1, e_{2,3}^2 = -1;$
4. $e_1^2 = 1, e_2^2 = 1, e_3^2 = 1, e_{1,2}^2 = 1, e_{1,3}^2 = -1, e_{2,3}^2 = -1;$
5. $e_1^2 = 1, e_2^2 = 1, e_3^2 = 1, e_{12}^2 = -1, e_{13}^2 = -1, e_{23}^2 = -1.$

Выбранные комбинации гарантируют восстановление исходного сообщения при осуществлении некоммутативного умножения.

Построим таблицу умножения для восьмимерных чисел на базе алгебры Клиффорда. Пусть базисные элементы e_1^2, e_2^2, $e_{1,2}^2$, $e_{1,3}^2$, $e_{2,3}^2$ алгебры Клиффорда равны (-1, -1, -1, -1, -1), тогда элементы таблицы будут иметь следующие значения, которые отражены в таблице 2.

Таблица 2. Таблица умножения с базисными элементами алгебры Клиффорда (-1, -1, -1, -1, -1)

•	e_0	e_1	e_2	e_3	$e_{1,2}$	$e_{1,3}$	$e_{2,3}$	$e_{1,2,3}$
e_0	1	e_1	e_2	e_3	$e_{1,2}$	$e_{1,3}$	$e_{2,3}$	$e_{1,2,3}$
e_1	e_1	-1	$e_{1,2}$	$e_{1,3}$	$-e_2$	$-e_3$	$e_{1,2,3}$	$-e_{2,3}$
e_2	e_2	$-e_{1,2}$	-1	$e_{2,3}$	e_1	$-e_{1,2,3}$	$-e_3$	$e_{1,3}$
e_3	e_3	$-e_{1,3}$	$-e_{2,3}$	-1	$e_{1,2,3}$	e_1	e_2	$-e_{1,2}$
$e_{1,2}$	$e_{1,2}$	e_2	$-e_1$	$e_{1,2,3}$	-1	$e_{2,3}$	$-e_{1,3}$	$-e_3$
$e_{1,3}$	$e_{1,3}$	e_3	$-e_{1,2,3}$	$-e_1$	$-e_{2,3}$	-1	$e_{1,2}$	e_2
$e_{2,3}$	$e_{2,3}$	$e_{1,2,3}$	e_3	$-e_2$	$e_{1,3}$	$-e_{1,2}$	-1	$-e_1$
$e_{1,2,3}$	$e_{1,2,3}$	$-e_{2,3}$	$e_{1,3}$	$-e_{1,2}$	$-e_3$	e_2	$-e_1$	1

2.4 Шестнадцатимерные числа как элементы группы

Для шестадцатимерных чисел возможно построить 1024 различных таблиц умножения на базе алгебры Клиффорда (1022 некоммутативных).

Для примера выбрана следующая комбинация базисных элементов алгебры Клиффорда, которая гарантирует восстановление исходного сообщения при осуществлении некоммутативного умножения:

$e_1^2 = 1$; $e_2^2 = 1$; $e_3^2 = 1$; $e_4^2 = 1$; $e_{1,2}^2 = -1$; $e_{1,3}^2 = -1$; $e_{1,4}^2 = -1$; $e_{2,3}^2 = -1$; $e_{4,3}^2 = -1$; $e_{3,4}^2 = 1$.

2.5 Реализация шифрования на четырехмерной алгебре Клиффорда

Рассмотрим пример реализации предложенного способа шифрования сообщения с последующей его расшифровкой на четырехмерной алгебре Клиффорда с базисными элементами (-1, -1, -1). Таблица умножения базисных единиц алгебры имеет вид согласно таблицы 1.

Элементы соответствующей алгебры зададим над простым полем Галуа характеристики p, то есть $F = GF(p)$.

Выбираем простые числа $p = 17$ и $q = 19$. Вычислим их произведение: $N = 323$.

Генерируем две циклические подгруппы G_1 и G_2 с максимальными периодами $v = w = p^2-1$, $G_1 \neq G_2$.

Выбираем ключ шифрования $e = 23$ - взаимно-простое с v.

Определив все различные периоды некоммутативных примитивов, найдем наименьший общий делитель для них. Это число равно $N_1 = 465585120$.

По входным параметрам базисных элементов (-1 -1 -1) построим таблицу умножения, которая является некоммутативной и выберем некоторый некоммутативный примитив $q = 149 + 101i + 229j + 227k$. Найдем для q обратный элемент $q^{-1} = 291 + 297i + 21j + 207k$.

Из группы G_2 выберем произвольный элемент M в качестве исходного сообщения $M = 116 + 101i + 120j + 116k$.

Передающая сторона формирует зашифрованное сообщение $C = q * m^e * q^{-1} = 203 + 150i + 89j + 215k$.

Принимающая сторона определяет секретный ключ дешифрования d = 263156807, который является взаимно обратным с e по модулю N_1 и расшифровывает сообщение $m = q^{-1} * C^d * q = 116 + 101i + 120j + 116k$.

Сравнение вычисленного сообщения с исходным сообщением показывает, что криптограмма *C* расшифрована правильно, т.е. из нее получено исходное сообщение *M*.

2.6 Реализация шифрования на восьмимерной алгебре Клиффорда

Рассмотрим пример реализации предложенного способа шифрования сообщения с последующей его расшифровкой на восьмимерной алгебре Клиффорда, где размерность базиса dim $E = 2^d = 8$. Сам базис имеет вид (1,e_1,e_2,e_3,$e_{1,2}$,$e_{1,3}$,$e_{2,3}$,$e_{1,2,3}$).

Таблица умножения базисных единиц алгебры имеет вид согласно таблицы 2.

Элементы соответствующей алгебры зададим над простым полем Галуа характеристики *p*, то есть F = *GF(p).*

Выбираем простое число p = 11.

Генерируем две циклические подгруппы G_1 и G_2 с максимальными периодами $v = w = p^2-1 = 120$, $G_1 \neq G_2$.

Выбираем элемент секретного ключа *X* из подгруппы G_1: $X = (1\ 2\ 9\ 5\ 8\ 4\ 1\ 7)$.

Выбираем дополнительные ключи шифрования:

1) число e = 107 - взаимно-простое с v,
2) произвольное число y = 1, удовлетворяющее $1 \leq y < w$.

Из группы G_2 выберем произвольный элемент *M* в качестве исходного сообщения *M* = (2 2 1 10 9 10 3 8).

Передающая сторона формирует криптограмму С:

$C = X \bullet M^{107} \bullet X^{-1} = (2\ 5\ 3\ 5\ 2\ 7\ 2\ 10)$.

Принимающая сторона определяет дополнительный секретный ключ дешифрования d = 83, который вычисляется из условия $d = e^{-1}$ т.е. $e \bullet d \equiv 1 \pmod v$ и расшифровывает сообщение:

$M = X^{-1}\ Y_1^{83}\ X = (2\ 2\ 1\ 10\ 9\ 10\ 3\ 8)$.

Сравнение вычисленного сообщения с исходным сообщением показывает, что криптограмма *C* расшифрована правильно, т.е. из нее получено исходное сообщение *M*.

2.7 Оценка сложности способа шифрования

Ключевым моментом в процедуре шифрования и дешифрования данных являются свойства ассоциативности и унитарности конечных групп, а также наличие обратного элемента для ключа *X*. В этом случае всегда будет выполняться равенство $X \cdot X^{-1} = X^{-1} \cdot X = e$ и, следовательно, $M = X^{-1} \cdot (X \cdot M \cdot X^{-1}) \cdot X = X^{-1} \cdot C \cdot X = M$. Данное условие обеспечивает достоверное преобразование исходного сообщения в шифр и обратно.

Допустим, нам требуется вычислить параметры секретного ключа по известному исходному сообщению *G* и криптограмме *C*. Поскольку вычислить эти два неизвестных элемента по отдельности нельзя, то эта задача не сводится к задаче дискретного логарифмирования в циклической подгруппе. Нахождение неизвестных *G* и *e* по значениям *Y* и *G* представляет собой самостоятельную трудную задачу, отличную от задачи дискретного логарифмирования. При известном значении X можно вычислить $Y' = X^{-1} \cdot Y \cdot X$ или $G' = X \cdot G \cdot X^{-1}$, после чего число X можно найти из уравнения $Y' = G^x$ или из уравнения $Y = G^{\alpha}$ соответственно, т.е. решая задачу дискретного логарифмирования. Однако значение *X* является неизвестным, поэтому задача дискретного логарифмирования в циклической подгруппе в явном виде не стоит.

Криптографическая стойкость алгоритма определяется на основе числа возможных некоммутативных элементов, значения, до которого производилась операция некоммутативного умножения в поисках обратного элемента для каждого выбранного некоммутативного примитива и числа некоммутативных таблиц умножения для выбранного числа.

3. Заключение

В данной работе рассмотрен подход в области криптографической защиты информации на примере криптосистемы с открытым ключом, позволяющий при меньших значениях ключа достигать большей криптографической стойкости шифруемого сообщения. Метод достигается путем использования некоммутативных конечных групп, основанных на свойствах алгебры Клиффорда. Алгеброй Клиффорда в данном алгоритме задается правило генерирования элементов группы, а также правило выполнения групповой операции умножения.

Предложенный способ шифрования имеет в основе трудную задачу с доказанной экспоненциальной сложностью в отличие от задач дискретного логарифмирования и факторизации. В основе данной криптосистемы использована трудная задача нахождения сопрягающего элемента в некоммутативных группах, на которой строится разработанный алгоритм с открытым распределением ключей.

Благодарности

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 15-07-99514.

Работа выполнена при финансовой поддержке Министерства образования и науки РФ (проект № 2.2226.2017/ПЧ), при финансовой поддержке Минобрнауки России (договор № 02.G25.31.0204) в рамках реализации Постановления Правительства РФ № 218 «О мерах государственной поддержки развития кооперации российских образовательных организаций высшего образования, государственных научных учреждений и организаций, реализующих комплексные проекты по созданию высокотехнологичного производства», при финансовой поддержке проектов в рамках госконтрактов №02.G25.31.0204, №2.9140.2017/БЧ, №2.2226.2017/ПЧ и гранта РФФИ №15-07-99514а.

Литература

[1] Announcing Request for Nominations for Public-Key Post-Quantum Cryptographic Algorithms [Electronic resource]. — Access mode: https://www.federalregister.gov/documents/2016/12/20/2016-30615/announcing-request-for-nominations-for-public-key-post-quantum-cryptographic-algorithms (06.02.2017).

[2] NIST Asks Public to Help Future-Proof Electronic Information [Electronic resource]. — Access mode: https://www.nist.gov/news-events/news/2016/12/nist-asks-public-help-future-proof-electronic-information (06.02.2017).

[3] Молдовян, Н.А. Теоретический минимум и алгоритмы цифровой подписи / Н. А. Молдовян. - СПб.: Издательство БХВ-Петербург, 2010. – 304 с.

[4] Широков, Д. С. Лекции по алгебрам Клиффорда и спинорам / Д. С. Широков. – М.: МИАН, 2012. – 180 с.